British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 7, Issue 2, 2024 (pp. 35-42)
www.abjournals.org

USING QR CODE AND A SMARTPHONE TO PROVIDE UNIVERSITY OF CROSS RIVER STATE (UNICROSS) CERTIFICATE AUTHENTICATION

Umoh Enoima Essien

Department of Computer Science, University of Cross River State.

Email: enoimaumoh@unicross.edu.ng

Cite this article:

Umoh Enoima Essien (2024), Using QR Code and a Smartphone to Provide University of Cross River State (UNICROSS) Certificate Authentication. British Journal of Computer, Networking and Information Technology 7(2), 35-42. DOI: 10.52589/BJCNIT-WAD9E7IE

Manuscript History

Received: 16 Mar 2024

Accepted: 15 May 2024

Published: 19 Jun 2024

ABSTRACT: *In the modern world, people frequently fabricate their credentials in order to secure a job or to show up where and when it is necessary. Verification is the most effective approach to identify those fraudulent certificates. Despite this, the paper verification method requires a drawn-out and time-consuming process to handle certificate verification because the certificates must be returned to the institutions who awarded them. As a result, the certificates either fail to pass verification or are delayed by the lengthy process. Hence, a certificate verification method using QR codes is developed in this study for quick verification of University of Cross River State (UNICROSS) certificate genuineness. A Smartphone and 3D Printed QR Code were employed for the enhancement of UNICROSS certificate mobile authentication services. ScanTrust anti-counterfeiting services were used to secure and host the encrypted information. Results show that our framework is effective for creating mobile authentication services with high user satisfaction rate and having reasonably low computing requirements.*

KEYWORDS: Quick Response Code, UNICROSS, Certificate, Authentication, Verification, Certificate Holder, Scanning, Encrypted, Decrypted, Smartphone.

Article DOI: 10.52589/BJCNIT-WAD9E7IE
DOI URL: https://doi.org/10.52589/BJCNIT-WAD9E7IE

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 7, Issue 2, 2024 (pp. 35-42)

www.abjournals.org

INTRODUCTION

It is common for software systems to generate digital copies of certificates, which you can then print out and show or deliver digitally in some other way. But with so many tools available to create fake certificates, it can be difficult to ensure someone has the skill. Certificates are a great way to demonstrate skills learned, achievements made, and prove qualifications earned, though in our digital age, a piece of paper may not be enough for certificate verification. The development of technology has reduced the cost of copying and printing documents, which has encouraged fraud and degree certificate forgery. This art compromises both the integrity of the institution issuing the certificate as well as the integrity of the certificate holder [1]. This test of integrity can be avoided in UNICROSS by adopting and implementing the secured QR code on any certificate awarded by the university.

The proposed system aims to develop a system that will verify and authenticate the validity of a certificate issued by the UNICROSS, provide a database for the institution's certificate records, build a robust system that can operate for extended periods of time, develop a flexible system that can be altered depending on changing requirements, and develop a system that can increase operational efficiency. Attempts to use Information Technology have been questioned as universities would not allow third party organizations to access their verification database, as a result of which the verification process remains partially or entirely manual [2]. Quick Response code is a two-dimensional barcode that is usually used to encode bits of information represented as black square dots placed on a white square grid [3]. They are designed to decode the data quickly [4].

Therefore, the creation of a Quick Response Code and its integration into a UNICROSS certificate for verification will serve as the starting point for our research projects. Based on the references to the student's information printed on certificates, a secure QR code will be created. Furthermore, ScanTrust's mobile scanner will be used on mobile devices with the aid of a certain algorithm that will decrypt the QR Code in order to validate the certificates. Due to the securely embedded qualities produced by the system, this system will be created to allow only the authorized scanner to be able to decrypt and translate the QR-code.

LITERATURE REVIEW

Smartphones and tablets with cameras may be used to scan QR codes, which are two-dimensional barcodes. The QR code can be scanned by aiming the device's camera at it and making sure the whole code is inside the frame that appears on the screen. When the code is successfully scanned, it is identified and opened in a specific application, such as a web browser (Türker, 2022; Fu & Liu, 2019). A novel enhanced security method for QR code-based document identification was developed in 2016 (Revathi, Annapandi & Ramya, 2013). In order to eliminate fake certificates, this system uses biometric fingerprint scanners and QR readers to confirm the authenticity of the certificates. This solution focuses on using the user's fingerprint and an image of the certificate to create a QR code when it is in use. A novel Confidential Encrypted Data Hiding and Retrieval Using QR Authentication System was created by (Dey et al., 2013). Each student's name, roll number, registration number, semester and year of study, grades earned in various topics, and other pertinent information are all kept in a QR Code within this system. Although the QR code's content might change, in this

Article DOI: 10.52589/BJCNIT-WAD9E7IE
DOI URL: https://doi.org/10.52589/BJCNIT-WAD9E7IE

implementation it consists of a URL that is embedded and links to the certificate object that is kept in the issuer's database. Each certificate code is unique. The official authority's verification webpage, which may be accessed by loading the scanned URL and an SSL certificate (Wazan et al., 2009), can be accessed by loading the official URL, which is https://weryfikacja.pti.org.pl. All PTI/ECDL Poland-issued electronic certificates can now be authenticated thanks to this service. People can enter the certificate's unique code on the verification web page that loads via the QR code and click the "verify" button. The field containing the unique code is already filled in if the page was loaded by a QR scan, and the verification procedure can move forward.

Benefits of Adopting QR Codes

Today, electronic certificate verification is a crucial activity, and QR codes are widely used because of their advantages.

Adopting QR codes for certificate verification offers numerous benefits, including:

Enhanced Security: QR codes can contain encrypted information, making them difficult to forge or tamper with. This enhances the security of certificates, reducing the risk of fraud or counterfeit.

Ease of Verification: QR codes enable quick and easy verification of certificates using a smartphone or any device with a camera. This eliminates the need for manual verification processes, saving time and effort for both issuers and verifiers.

Accessibility: QR code-based verification can be easily accessed by anyone with a smartphone and a QR code reader app, making it accessible to a wide range of users without requiring specialized equipment or software.

Real-time Validation: QR code verification systems can provide real-time validation of certificates, allowing instant confirmation of their authenticity. This is particularly useful in situations where time is of the essence, such as verifying qualifications during job interviews or event registrations.

Reduced Administrative Burden: Automating certificate verification with QR codes reduces the administrative burden associated with manual verification processes. This frees up resources that can be allocated to other tasks, improving overall efficiency.

Cost Savings: Implementing QR code-based verification systems can lead to cost savings by streamlining verification processes and reducing the need for manual labor. It also helps in reducing the costs associated with fraud detection and prevention.

Traceability and Audit Trail: QR code-based verification systems can provide a digital trail of certificate verification activities, including who verified the certificate and when. This traceability enhances accountability and facilitates audit processes.

Flexibility and Scalability: QR code-based verification systems can be easily scaled to accommodate a large volume of certificates and users. They can also be customized to meet the specific needs of different organizations and industries.

Article DOI: 10.52589/BJCNIT-WAD9E7IE
DOI URL: https://doi.org/10.52589/BJCNIT-WAD9E7IE

Environmentally Friendly: By digitizing certificate verification processes, QR codes help reduce the need for paper-based certificates, contributing to environmental sustainability efforts by minimizing paper waste.

Improved User Experience: QR code-based verification offers a seamless and user-friendly experience for both certificate issuers and verifiers. It simplifies the verification process, reducing friction and improving overall user satisfaction.

Overall, adopting QR codes for certificate verification offers a secure, efficient, and cost-effective solution that enhances trust and reliability in the validity of certificates and credentials.

CONCEPTUAL MODEL FOR THE SUGGESTED SYSTEM

To the best of our knowledge, the suggested system in this study is the first system to be deployed for electronic authentication of UNICROSS Certificates, even though it shares many of the positive aspects of the previous initiatives. This is significant because it eliminates the manual method of certificate authentication.

Modules and Description

The proposed system has two modules which are: QR Generator module and QR Code Verification Module.

QR Generator Module

The administrator of the proposed system can enter certificate information such as Certificate Holder Name, Department, Matriculation Number, Class of Degree/Programme, Year of graduation, Passport photograph, etc into the application, which will then generate a QR code for the certificate. The system safely stores the certificate data in a database, guaranteeing data accessibility and integrity. People or organizations can easily authenticate certificates by scanning the QR code with a webcam or QR code scanner, which allows the system to retrieve the certificate details and verify its authenticity. This module's security is crucial to preventing illegal access and safeguarding user information. The system is protected by a number of security mechanisms.

Proposed Procedure for QR Code Generator Module

1. Enter the certificate holder information, such as Certificate Holder Name, Department, Matriculation Number, Class of Degree/Programme, Year of graduation, Passport photograph.

2. Obtain the encrypted QR code image.

3. Store the encrypted QR code image on the database.

4. The QR generator produces a QR code image which is printed at the bottom of every certificate issued by the university.

Article DOI: 10.52589/BJCNIT-WAD9E7IE
DOI URL: https://doi.org/10.52589/BJCNIT-WAD9E7IE

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 7, Issue 2, 2024 (pp. 35-42)

www.abjournals.org

QR Code Verification Module

This crucial module manages the QR code-based certificate verification process. One essential part of the "Certificate Authentication System using QR Code" is the "QR Code Verification Module." The purpose of this module is to enable verifiers to use QR code scanning to quickly and properly authenticate UNICROSS Certificates using commodity smartphone and QR code.

The module verifies the QR code to ascertain its legitimacy after it has been scanned. The verification procedure determines whether the QR code matches an authentic certificate in the system's database. To confirm authenticity, the module compares the data from the QR code with the information from the stored certificate. The system shows the certificate details, including the name and contact details of the certificate holder, along with an Authentic label if the QR code is authentic. The system shows a "Invalid QR Code" notice if the QR code is invalid (for example, it has expired, been altered, or is not present in the database).

Proposed Process for QR Code Verification Module

1. Open the smartphone app that you have installed for authentication.

2. Focus your smartphone camera on the QR code image at bottom of the certificate.

3. The app carried out verification on the Captured QR code image. This confirms whether the captured QR code image conforms with the QR code image on the database or not.

4. Decryption of the QR code captured hereby displaying the details of the certification holder on the smartphone screen.

Article DOI: 10.52589/BJCNIT-WAD9E7IE
DOI URL: https://doi.org/10.52589/BJCNIT-WAD9E7IE

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 7, Issue 2, 2024 (pp. 35-42)

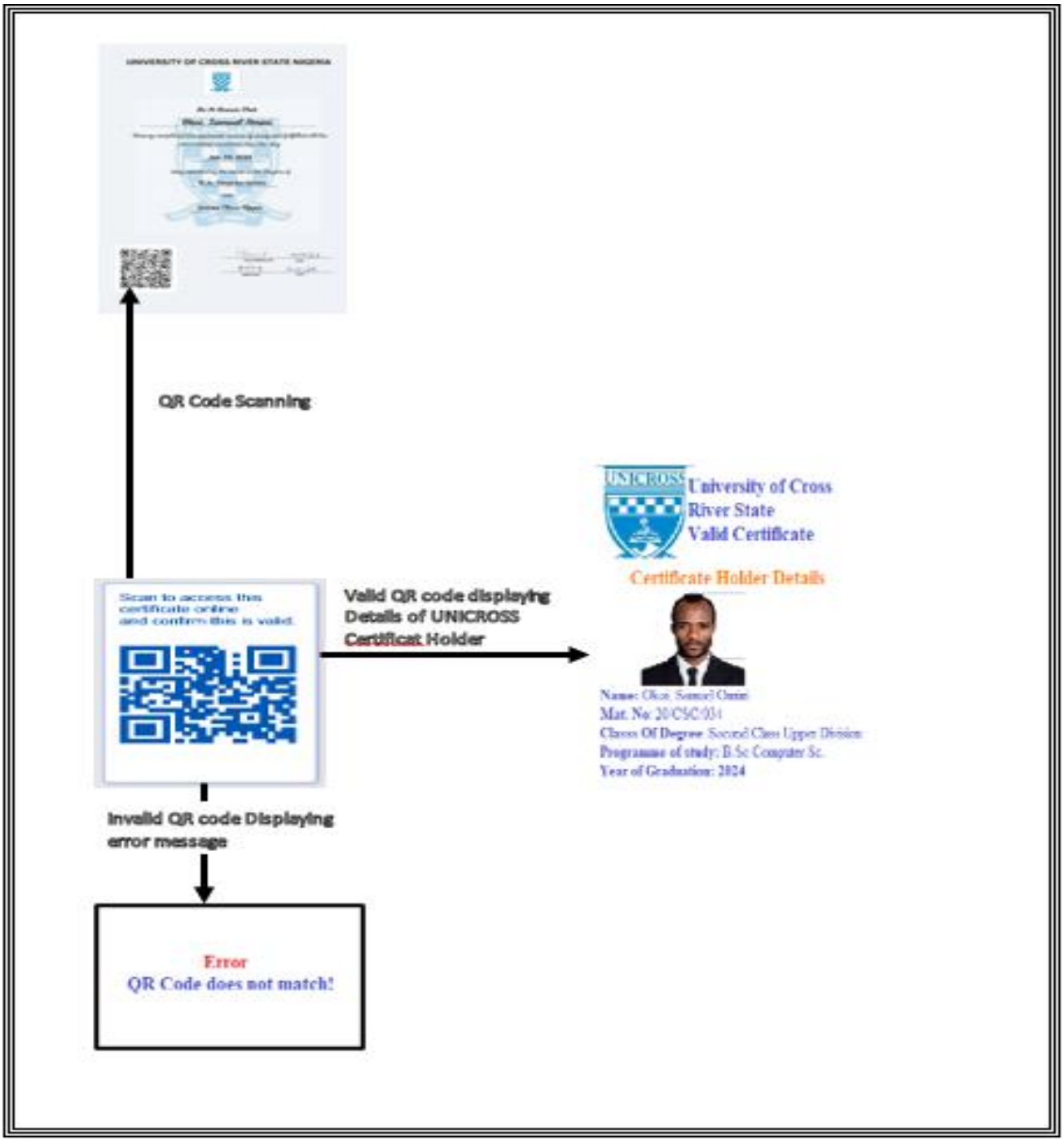

Figure 1. Screenshot Conceptual Framework of UNICROSS Certificate Authentication System

Article DOI: 10.52589/BJCNIT-WAD9E7IE
DOI URL: https://doi.org/10.52589/BJCNIT-WAD9E7IE

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 7, Issue 2, 2024 (pp. 35-42)
www.abjournals.org

EXPERIMENTAL RESULTS

Ten distinct UNICROSS certificates were created and verified using the suggested architecture. Table 1 displays the conditions under which the experiment was conducted, and Table 2 displays the outcomes. Two conditions were applied to the smartphone that was utilized for authentication: with the flash light on and off.

Table 1: Experimental Parameters

S/N	Parameters	Values
1.	Smallest QR Code Image Size	21 x 21 Modules
2.	Largest QR Code Image Size	177 x 177 Modules
3.	Maximum data capacity	Numeric 7089 Characters
		Alphanumeric 4096 Characters
		Binary 2953 Bytes
		Kanji 1718 Charaters
4	Smart Phone	OPPO A54

Table 2: Experimental Results

	Authentication Duration	
Certificate	Flash Light (Off	Flash Light (On
Cert. 1	7	4
Cert. 2	3	1
Cert. 3	5	2
Cert. 4	9	4
Cert. 5	6	2
Cert. 6	2	1
Cert. 7	9	4
Cert. 8	8	3
Cert. 9	7	2
Cert. 10	5	2
Average	6.1	2.5

Results Analysis

Results from the experiment showed that our system operates more quickly in high illumination. Table 2 displays the average time to authenticate a certificate with the smart phone flash light on, which is 2.5 seconds, compared to 6.1 seconds without flash. This is because higher illumination in this context improves clarity, meaning that when the QR code is clearly displayed, the smart phone's embedded QR reader can capture expected data more quickly.

Article DOI: 10.52589/BJCNIT-WAD9E7IE
DOI URL: https://doi.org/10.52589/BJCNIT-WAD9E7IE

CONCLUSION

The suggested approach makes the process of verifying a UNICROSS degree certificate easier by means of a smartphone and QR Code. It has produced a functioning prototype that authenticates a degree certificate from the university database, in real time. You can also easily obtain insight details about a certificate holder from the university by connecting to the database.

Ten printed certificates were utilized to test our technique, which leads to speedier authentication when the smartphone's camera flash is turned on as opposed to off. The module verifies the QR code to ascertain its legitimacy after it has been scanned. The verification procedure determines whether the QR code matches an authentic certificate in the system's database. To confirm authenticity, the module compares the data from the QR code with the information from the stored certificate. The system shows the certificate details, including the name and passport photograph of the certificate holder, if the QR code is valid. The system shows an "Invalid QR Code" notification if the QR code has been altered or is not present in the database.

REFERENCES

[1] Umoh Enoima Essien and Ofut Ogar Tumenayu (2022). University of Cross River State Certificate Verification System With Embedded Unclonable Quick Response Code Digital Signature. Journal of Contemporary Research (JOCRES) VOL. 1 (2) PP 48-55.

[2] Boukar, Moussa Muslu, Isa Yusuf and Salisu (2017). "A Web Service Based Database access for Nigerian Universities' Certificate Verification System", International Journal of Computer Techniques pp 1-7.

[3] Uzun, V., & Bilgin, S, (2016). "Evaluation and implementation of QR Code Identity Tag system for Healthcare in Turkey".Springer Plus. https://doi.org/10.1186/s40064-01630209,

[4] Pons, D, (2011). "QR code in use: the experience at the UOV library", Serials-24 (3), 47-56,

[5] Türker, Altay, Okumuş (2022) "Understanding user acceptance of QR code mobile payment systems in Turkey: An extended TAM." In Technological Forecasting and Social Change, 184, 121968.

[6] Fu, Cheng, Liu, Yu (2019) "A new two-level information protection scheme based on visual cryptography and QR code with multiple decryptions.", in Measurement, 141, 267–276.

[7] Revathi M K, Annapandi P, Ramya K P. (2013). Enhancing Security in Identity Documents Using QR Code. International Journal of Research in Engineering & Advanced Technology.

[8] Somdip Dey, Asoke Nath, Shalabh Agarwal. (2013). Confidential Encrypted Data Hiding and Retrieval Using QR Authentication System. IEEE International Conference on Communication Systems and Network Technologies (CSNT).

[9] Wazan, Laborde, Chadwick, Barrere, and Benzekri (2009) "Which web browsers process ssl certificates in a standardized way?.", in Emerging Challenges for Security, Privacy and Trust: 24th IFIP TC 11 International Information Security Conference, SEC 2009, Pafos, Cyprus, May 18–20, 2009. Proceedings 24 (pp. 432-442). Springer Berlin Heidelberg.

Article DOI: 10.52589/BJCNIT-WAD9E7IE
DOI URL: https://doi.org/10.52589/BJCNIT-WAD9E7IE